UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
AIKEN DIVISION

SHANNON DUNN, individually and on behalf of all others similarly situated, PLAINTIFF, v. SRP FEDERAL CREDIT UNION, DEFENDANT.	1:24-cv-07684-CMC CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL ENCLOSED

INTRODUCTION

1. This case arises from a data breach. Defendant SRP Federal Credit Union (hereafter "SRP") is a credit union that, as part of its normal business operations collects highly sensitive data about its clients including social security numbers, financial information, and other details. SRP's customers have no choice but to trust SRP to keep their data secure.

2. In a story that has become all too familiar, an unauthorized third-party gained access to SRP's network beginning on September 5, 2024, and absconded with personally identifying information (hereafter, "PII"), including highly sensitive financial information. Criminals can now sell the victims' data on the black market for the purpose of stealing their identities. None of this would have occurred if SRP had implemented reasonable data security measures.

3. Plaintiff Shannon Dunn was a victim of the data breach. She brings this action on behalf of herself and all others similarly situated, seeking damages for the injuries that Defendant's

negligence have and will cause, as well as injunctive relief to ensure that the data Defendant continues to store will be protected by reasonable data security practices going forward.

PARTIES

4. Plaintiff Shannon Dunn is a resident of Harlem, Georgia, where she intends to remain.

5. Defendant SRP is a federally chartered and regulated credit union, with its principal place of business at 1070 Edgefield Road, North Augusta, SC 29860. On information and belief, a substantial portion of the relevant acts giving rise to this lawsuit took place at SRP's corporate headquarters.

JURISDICTION AND VENUE

6. This Court had personal jurisdiction over SRP because its principal place of business is (and at all relevant times was) located in North Augusta, South Carolina, in this District.

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) because at least one member of the class, including Plaintiff Dunn, is a citizen of a state different from SRP; the amount in controversy exceeds $5,000,000, exclusive of interests and costs; the proposed class consists of more than 100 members, and not of the exceptions under the subsection apply to this action.

8. Venue is proper in this District, and in this Division, because SRP's principal place of business is in Aiken County, South Carolina. *See* 28 U.S.C. §1391(b)(1); Local Civ. Rule 3.01(A)(1).

FACTUAL ALLEGATIONS

A. SRP allowed Dunn's data to be stolen.

9. According to the data breach notice that Dunn received, an unauthorized third-party gained remote access to SRP's network beginning on September 5, 2024, and continuing through

November 4, 2024, acquired information from Plaintiff and Class members. A true and correct copy of the Notice Letter is attached as Exhibit 1.

10. Based on the disclosures in the Notice, information pertaining to Plaintiff and Class members was part of the data acquired by an unauthorized external party in the Data Breach.

11. The specific information that was acquired includes: name, date of birth, Social Security Number, and SRP account number. Exhibit 1, at 1.

12. Because this data breach targeted financial and personally identifying information, it is reasonable to infer that the hackers will use victims' data for fraudulent purposes, including identity theft.

13. Since discovering the Data Breach, SRP has "taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical measures." Exhibit 1, at 1. Either such actions are meaningless window-dressing, and are therefore of no help whatsoever, or they are actually effective – which means that they should have been employed in the first place in order to have prevented or limited the impact of the Data Breach. It will take discovery to determine which it is here.

14. Weeks after the Data Breach was discovered and law enforcement was notified, SRP publicly announced the Data Breach and notified those of its customers who were placed at risk of identity theft. It also sent notices to various states' Attorneys General and to its customers whose PII was acquired by criminals in the Data Breach.

15. While claiming that "we have no reason to believe that your personal information has been misused," the Notice Letter Plaintiff received says that that Class members should obtain credit monitoring and identity theft protection services to help them detect possible misuse of PII. See Exhibit 1. Class members are therefore at a substantial risk of identity theft.

16. As a result of the Data Breach, Plaintiff and Class members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

B. The data breach was highly foreseeable, yet Defendant failed to take reasonable precautions.

17. Given the type of data that Defendants collected and stored, it was highly foreseeable that bad actors would attempt to access it without permission.

18. "[H]ackers are likely to be drawn to databases containing information which has a high value on secondary black markets," such as "identifying and financial data." Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 854–55 (2021). Consequently, "relevant and rational firms should engage in greater security investment and reduced collection—all steps to limit the prospects of a potential breach and subsequent notification." *Id*. at 855.

19. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

20. Because Defendant collected and stored identifying and financial information that is very valuable to criminals, it was highly foreseeable that a bad actor would attempt to access that data without permission.

21. On information and belief, Defendant frequently collects and stores personally identifying and financial information. Therefore, the burden (if any) of implementing reasonable

data security practices is minimal in comparison to the substantial and highly foreseeable risk of harm.

22. SPR is well aware of its duty to keep customers' information secure. Its privacy policy states "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law" including "computer safeguards and secured files and buildings. SRP Privacy Notice (accessed January 2, 2025), https://srpfcu.org/your-credit-union/policies/privacy-notice/.

23. On information and belief, Defendant failed to adequately train their employees on even the basic cybersecurity protocols, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of multi-factor authentication for all users;
b. Locking, encrypting and limiting access to computers and files containing sensitive information;
c. Implementing guidelines for maintaining and communicating sensitive data;
d. Protecting sensitive customer information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and
e. Providing focused cybersecurity awareness training programs for employees.

24. The FTC has noted the need to factor data security into all business decision-making. *Start With Security, A Guide for Business*, FTC (accessed June 9, 2022), https://bit.ly/3mHCGYz. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative

access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software. *Id.*

25. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the data breach, further clarify the measures businesses must take to meet their data security obligations.

26. As previously stated, SPR's own privacy policy acknowledges its obligation to conform with federal data security guidelines, including FTC standards.

27. On information and belief, Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and thousands of members of the proposed Classes to unscrupulous operators, con artists, and outright criminals.

28. On information and belief, Defendant violated its obligation to implement best practices and comply with industry standards concerning computer system security, which allowed class members' data to be accessed and stolen by criminals.

C. Dunn's information was exposed in the data breach, which caused her to suffer concrete injuries.

29. Plaintiff Shannon Dunn has been a banking customer of SRP for at least 10 years. As part of that banking relationship, Plaintiff necessarily provided her PII to SRP.

30. On December 26, 2024, Plaintiff Dunn received a data breach notification in the mail, informing her that her personally identifiable information, including financial information, was accessed in the breach.

31. Plaintiff's PII was compromised in the data breach and was likely stolen and in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII.

32. Defendant continues to maintain Plaintiff's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff would not have entrusted her PII to Defendant SRP had she known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

33. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

34. As a result of the data breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the data breach, Plaintiff has spent significant time monitoring her accounts and credit score and has sustained emotional distress in addition to her lost time. This is time that was lost and unproductive and took away from other activities and duties.

35. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that he entrusted to Defendant SRP—which was compromised in and as a result of the data breach

36. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the data breach and has anxiety and increased concerns for the loss of her privacy.

37. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number and financial information, being placed in the hands of criminals.

38. Indeed, on at least two occasions in November and December of 2024, unidentified individuals attempted to access credit by using Plaintiff Dunn's information. While these attempts were not ultimately successful, it highlights that the concerns about identity theft are not merely hypothetical concerns but have actually come to pass.

39. Prior to receiving the data breach notice in late December 2024, Plaintiff had no way of connecting the access attempts on her credit to SRP. As such, many similarly situated

Class members may have experienced identity theft incidents in late 2024 that they had no way of knowing were in fact connected to SRP's data breach.

40. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the data breach. As a result of the data breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

41. Because personally identifying and financial information has been accessed by criminals, Plaintiff and the Class have suffered concrete and ongoing injuries.

42. Plaintiff and the Class are at an imminent and substantial risk of identity theft.

43. According to experts, one out of four data breach notification recipients become a victim of identity fraud. Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims, THREATPOST.COM (Feb. 21, 2013), https://bit.ly/3zB8Uwv.

44. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to $1,000.00 depending on the type of information obtained. See Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN (Dec. 15, 2017), https://bit.ly/2Ox2SGY.

45. The value of Plaintiff and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

46. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

47. One such example of criminals using PII for profit is the development of "Fullz" packages. "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://bit.ly/3Qj2eJd.

48. Cyber-criminals can cross-reference two sources of PII to marry unregulated or partial data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete "Fullz" dossiers on individuals.

49. The development of "Fullz" packages means that stolen PHI from the data breach can easily be used to link and identify it to Plaintiff's and the proposed Classes' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the data breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam

telemarketers) over and over. That is likely what is already happening to Plaintiff and members of the proposed Classes, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Classes' stolen PII is being misused, and that such misuse is fairly traceable to the data breach.

50. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

51. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

52. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

53. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

54. Moreover, the breach has diminished the value of Plaintiff and the Class's personal information.

55. The FTC has recognized that consumer data is a new and valuable form of currency. In a FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most

consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency." *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtabl*e, FTC (Dec. 7, 2009), https://bit.ly/3xKfzmu.

56. Since it was included in the breach, Plaintiff and the Class's information has already been accessed by criminals, which decreases its value in the marketplace.

57. Therefore, the value of Plaintiff and the Class's personal information was reduced by the data breach.

58. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

59. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

60. None of those injuries would have occurred if Defendant had implemented reasonable data security practices.

CLASS ACTION ALLEGATIONS

61. Pursuant to FED. R. CIV. P. 23(b)(2) and (b)(3), Plaintiff seeks certification of a Class defined as follows:

> All SRP customers whose personal information was compromised in connection with the data breach occurring on or around September 5, 2024.

62. Excluded from the Class are: (a) Defendant and its officers, directors, legal representatives, successors and wholly or partly owned subsidiaries or affiliated companies; (b) class counsel and their employees; and (c) the judicial officers and their immediate family members and associated court staff assigned to this case.

63. *Ascertainability*. The Class can be readily identified through SRP's records, which is demonstrated by the fact that many class members have already been identified and sent notice letters regarding the data breach.

64. *Numerosity*. SRP has reported to state regulators that the data breach affected approximately 240,000 individuals. Therefore, the Class is so numerous that individual joinder is impracticable.

65. *Typicality*. Plaintiff's claims are typical of the Class she seeks to represent. Like all class members, Plaintiff's personal information was exposed in the data breach as a result of Defendant's failure to implement reasonable data security measures. Thus, Plaintiff's claims arise out of the same conduct and are based on the same legal theories as those of the absent class members.

66. *Adequacy of Class Representative*. Plaintiff will fairly and adequately protect the interests of the Classes. She is aware of her fiduciary duties to absent class members and is determined to faithfully discharge her responsibility. Plaintiff's interests are aligned with (and not antagonistic to) the interests of the Class.

67. *Adequacy of Counsel*. In addition, Plaintiff has retained competent counsel with considerable experience in class action and other complex litigation, including data breach cases.

Plaintiff's counsel have done substantial work in identifying and investigating potential claims in this action, have considerable knowledge of the applicable law, and will devote the time and financial resources necessary to vigorously prosecute this action. They do not have any interests adverse to the Class.

68. *Commonality and Predominance*. This case presents numerous questions of law and fact with answers common to the Classes that predominate over questions affecting only individual class members. Those common questions include:

a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff and the Class's PII;

b. Whether Defendant breached the duty to use reasonable care to safeguard the Class's PII;

c. Whether Defendant breached its contractual promises to safeguard Plaintiff and the Class's PII;

d. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

f. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

g. Whether the data breach was caused by Defendant's inadequate cybersecurity measures, policies, procedures, and protocols;

h. Whether Defendant is liable for negligence, gross negligence, or recklessness;

i. Whether Defendant's conduct, practices, statements, and representations about the data breach of the PII violated applicable state laws;

j. Whether Plaintiff and the Class were injured as a proximate cause or result of the data breach;

k. What the proper measure of damages is; and

l. Whether Plaintiff and the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

69. *Superiority and Manageability.* A class action is superior to individual adjudications because joinder of all class members is impracticable, would create a risk of inconsistent or varying adjudications, and would impose an enormous burden on the judicial system. The amount-in-controversy for each individual class member is likely relatively small, which reinforces the superiority of representative litigation. As such, a class action presents far fewer management difficulties than individual adjudications, preserves the resources of the parties and the judiciary, and protects the rights of each class member.

70. *Injunctive or Declaratory Relief.* In addition, Defendant acted or failed to act on grounds that apply generally to the Class, such that final injunctive or declaratory relief as to any one class member is appropriate as to all class members.

CAUSES OF ACTION

Count 1: Negligence

71. Plaintiff incorporates by reference the allegations set forth in Paragraphs 1-70.

72. Plaintiff brings this count on her own behalf and on behalf of the Class.

73. Plaintiff and the Class entrusted their PII to financial institutions who turned that information over to Defendant. Knowing this, Defendant owed to Plaintiff and other the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the

information from the data breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

74. Defendant owed a duty of care to Plaintiff and the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the data breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and the Class's PII failing to properly supervise both the manner in which the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

75. Defendant owed these duties to Plaintiff and the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and the Class's personal and financial information in the conduct of its business, and Defendants retained that information.

76. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII.

77. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

78. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and

the Class, which actually and proximately caused the data breach and Plaintiff and the Class's injury.

79. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and the Class's actual, tangible, injury-in-fact and damages, including, without limitation, theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach.

Count 2: Negligence *Per Se*

80. Plaintiff incorporates by reference the allegations set forth in Paragraphs 1-70.

81. Plaintiff brings this count on her own behalf and on behalf of the Class.

82. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

83. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

84. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its customers' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences

of a data breach, including, specifically, the immense damages that would result to its customers in the event of a breach, which ultimately came to pass.

85. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

86. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

87. Defendant breached its duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

88. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

89. As a direct and proximate result, Plaintiff suffered actual losses and damages, including, without limitation, theft of her PII by criminals, improper disclosure of her PII, lost value of her PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence.

Count 3: Breach of Implied Contract

90. Plaintiff incorporates by reference the allegations set forth in Paragraphs 1-70.

91. Plaintiff brings this count on her own behalf and on behalf of the Class.

92. Defendant offered financial services to Plaintiff and members of the Class in return for their PII.

93. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects from customers to unauthorized persons. Defendant also promised to safeguard customer PII.

94. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for receiving financial services from Defendant.

95. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

96. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

97. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

98. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

99. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement.

Count 4: Unjust Enrichment

100. Plaintiff incorporates by reference the allegations set forth in Paragraphs 1-70.

101. Plaintiff brings this count on her own behalf and on behalf of the Class. Plaintiff pleads this count in the alternative to Count 3.

102. Plaintiff and the Class conferred a benefit on SRP in the form of service fees. SRP also benefitted from the receipt of Plaintiff and the Class's PII, as this was used for SRP's commercial purposes.

103. SRP knew of the benefits conferred on it by Plaintiff and the Class.

104. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class's services and their PII because SRP failed to adequately protect their PII. Plaintiff and the Class would not have provided their PII to SRP if they had known SRP would not adequately protect their PII.

105. SRP should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds it received due to its misconduct.

PRAYER FOR RELIEF

106. Plaintiff, individually and on behalf of all others similarly situated, hereby demands:

a. Certification of the proposed Class;

b. Appointment of the undersigned counsel as class counsel;

c. An award of all damages, including attorneys' fees and reimbursement of litigation expenses, recoverable under applicable law;

d. Restitution or disgorgement of all ill-gotten gains; and

e. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

107. Plaintiff demands a jury trial on all applicable claims.

Dated: January 13, 2025

DAVE MAXFIELD, ATTORNEY, LLC

s/ David A. Maxfield

David A. Maxfield, Fed, ID No. 6293
SOCO 80808 Building
808 D Lady Street
Columbia, SC 29201
Tel: (803) 509-6800
Fax: (855) 299-1656
Email: dave@consumerlawsc.com

BRONSTEIN, GEWIRTZ & GROSSMAN, LLC
Michael J. Boyle, Jr. (*pro hac vice* to be filed)
4200 Regent Street, Suite 200
Columbus, OH 43219
Tel: (614) 578-5582
Email: mboyle@bgandg.com

Peretz Bronstein (*pro hac vice* to be filed)
60 East 42nd Street, Suite 4600
New York, NY 10165
Tel: (212) 697-6484
Fax: (212) 697-7296
Email: peretz@bgandg.com

Counsel Plaintiff Shannon Dunn and for the Class